describes the above-noted blinding technique, in which a two-part value (M1, M2) is derived such that M1 XOR M2 corresponds to the original message M. It is not apparent from the Office Action what subject matter in this passage is considered to correspond to the claimed "manipulating means". Of particular significance, claim 11 recites that the manipulating means have "complementary input and/or output data relative to one another." There is no disclosure at column 2, lines 25-37 of a plurality of manipulating means that have input and/or output data that are respectively complementary to one another. Nor does the Office Action identify how this portion of the patent might be interpreted to disclose such subject matter.

For at least this reason, therefore, it is respectfully submitted that the Office Action has not shown that the Kocher patent "anticipates" the subject matter of claim 11. If the rejection is not withdrawn, the Examiner is respectfully requested to identify what subject matter, i.e. structure or operation, is considered to be the plurality of manipulating means having complementary input and/or output data relative to one another.

Claim 11 further recites a means for generating a random value that designates at least one of the manipulating means to be employed during a given execution of the cryptography technique. In connection with this subject matter, the Office Action refers to the Kocher patent at column 6, lines 39-67. In relevant part, this portion of the patent discloses that a random value K1 is produced. This random value comprises one part of the two-part blinded value for a key K. There is no disclosure that this random value functions to "designate" at least one of the manipulating means to be employed during a given execution of the DES algorithm. Rather, this random value, or a random permutation thereof, is employed as the key in the cryptographic operations. It does not perform any type of "designating" function.

For this additional reason, it is submitted that the Kocher patent does not anticipate the subject matter of claim 11. If the rejection is not withdrawn, the Examiner is respectfully

requested to identify which random value is being relied upon in the disclosure at column 6, lines 39-67, and where the patent teaches that such a random value designates at least one of the manipulating means that is identified in response to the first request set forth above. In the absence of such showings, it is respectfully submitted that the rejection cannot be maintained.

Claim 12 recites that the plurality of manipulating means each comprise a table of constants. In connection with this subject matter, the Office Action refers to the Kocher patent at column 7, lines 15-65. This portion of the patent discloses the creation of various tables. However, the Office Action does not identify any relationship between these tables and the "manipulating means" that is alleged to be disclosed at column 2, lines 21-36. These tables pertain to the initialization phase of the DES algorithm, and not to the "blinding" of the original message and/or the keys as described in the cited passage from column 2.

Claim 14 recites that the random value has first and second states. The first state designates a manipulating means that is employed during all of the rounds of the DES algorithm, whereas the second state designates at least two other manipulating means that are employed during different respective rounds of the algorithm. In connection with this subject matter, the Office Action refers to the Kocher patent at column 2, line 25 to column 3, line 9. This portion of the patent discloses that the S tables employed during the DES algorithm can also be stored in blinded form. However, the Office Action does not identify how this disclosure relates to the two states of the random value recited in claim 14.

Claims 1-8 were rejected under 35 U.S.C. §103, as being unpatentable over the Kocher patent in view of the Leppek et al patent (US 5,933,501). The first step recited in claim 1 is that of forming a group comprising at least the first three rounds of the cryptographic algorithm, and another ground comprising at least the last three rounds of the algorithm. The Office Action asserts that the Kocher patent discloses this subject matter at column 9, lines 14-17. This portion of the patent states that a transformation of the

message, and/or the key, can be performed at any time before results are required from the algorithm. It is not seen how this disclosure can be interpreted to suggest forming at least two groups, each comprising at least three rounds of the cryptographic algorithm. The Examiner is respectfully requested to explain how the patent is being interpreted to suggest the claimed subject matter.

The second step of claim 1 is that of applying a first sequence that uses a first manipulating means or a second sequence that uses other manipulating means in at least certain rounds of each group. This step further recites that the first and second sequences are such that "they supply the same result at the output from the last round in each group for the same given input message." The Office Action acknowledges that the Kocher patent does not disclose the subject matter, and relies upon the Leppek patent, particularly at column 4, lines 7-51. This portion of the patent does not disclose the use of first and second sequences that each supply the same result for the same given input message. Rather, it discloses a compound encryption scheme in which a plurality of different types of encryption routines are successively applied to data that is to be encrypted. As disclosed in the patent, each individual encryption routine can be a conventional encryption operator, "such as, PGP, DES, etc. routines." There is no suggestion in the patent that each of these routines produces the same output result for a given input message. Rather, because they are entirely different encryption techniques, they would be expected to produce *different* output results.

Consequently, even if the teachings of the Leppek patent were applied to the technique of the Kocher patent, the resulting combination would not lead a person of ordinary skill to the claimed subject matter. Whether considered individually or in combination, the patents do not disclose the claimed steps of forming a group comprising at least three rounds of the cryptographic algorithm and another group comprising at least the last three rounds of the algorithm, and for each of these groups selectively applying a first

sequence or a second sequence, each of which provides the same output result from the last round in each group for the same given input message.

In addition to these fundamental differences, other distinguishing features of the invention are recited in the dependent claims. For example, claim 2 recites that the respective manipulating means are such that they have complementary input and/or output data from one another. As discussed previously in connection with claim 11, the Kocher patent does not disclose such subject matter.

For at least the foregoing reasons, it is respectfully submitted that the Kocher patent does not anticipate the subject matter of claims 11-15, nor does it suggest the subject matter of claims 1-8, even when considered in combination with the Leppek patent. If the rejections are not withdrawn, the Examiner is respectfully requested to explain, with particularity, how the references are being interpreted to disclose the distinguishing features identified in the foregoing remarks.

Applicants would like to call the Examiner's attention to co-pending, related Application No. 09/807,607, filed June 1, 2001, which is being handled by a different Examiner. Since the Office Action in the present application cites the same prior art references as those cited in the related application, it appears that the Examiner may already be aware of that related application. However, the related application is being identified herein to confirm that the Examiner is aware of it.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: December 30, 2005

By: _____

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620